Some Theorems in Numbers.

By O. H. Mitchell,

Fellow in the Johns Hopkins University.

---

§1. *On the Residues mod. k of the Symmetric Functions of the Numbers less than k, where k = any Integer.*

In the following $\equiv$ will denote identical congruity, *i. e.*, $\phi(x) \equiv \psi(x)$, mod. k, will denote that the coefficients of corresponding powers of x are respectively congruous to one another mod. k. If $\Pi(x-\alpha)$ denote the product $(x-1)(x-2)\cdot(x-3)\ldots.(x-a+1)$, where a is a prime number, we know that $\Pi(x-\alpha) \equiv x^{a-1}-1$ mod. a. This expresses the fact that the symmetric functions $\Sigma\alpha$, $\Sigma\alpha\beta$, $\Sigma\alpha\beta\gamma$, &c. of the numbers less than (and prime to) a are each $\equiv 0$ mod. a, except the last, which is $\equiv -1$ mod. a. It is proposed in this section to determine the value of $\Pi(x-\alpha)$ for any integer, k, $= a^t b^u \ldots g^v h^w \ldots q^z$, where a, b, &c. are prime numbers; or, more generally, to determine the residue, mod. k, of $\Pi(x-\theta_s)$, where θ_s', θ_s'', θ_s''', &c. are those numbers less than k which contain $s = hi\ldots q$, and no prime factor of k not found in s. These numbers were called in my former paper, Vol. 3, No. 4, of this Journal, the s-totitives of k. The number of them was called the s-totient of k, and denoted by $\tau_s(k)$. It was there seen that $\tau_s(k) = a^{t-1}b^{u-1}\ldots q^{z-1}(a-1)(b-1)\ldots(g-1)$.

Theorem I. If $\Pi_{a^t}(x-\theta_1)$ denote the product $(x-\theta_1')(x-\theta_1'')(x-\theta_1''')\ldots$, where the numbers θ_1 are the prime totitives of a^t, a being an odd prime number, then

$$\Pi_{a^t}(x-\theta_1) \equiv (x^{a-1}-1)^{a^{t-1}} \text{ mod. } a^t;$$

and if θ_a', θ_a'', &c. be the a-totitives of a^t, then

$$\Pi_{a^t}(x-\theta_a) \equiv x^{a^{t-1}} \text{ mod. } a^t.$$

To prove the theorem it will be shown first that

$$\Pi_{a^t}(x-\theta_1) \equiv [\Pi_{a^{t-1}}(x-\theta_1)]^a \text{ mod. } a^t.$$

Let $\alpha, \beta, \gamma, \ldots \omega$ be the prime totitives of a^{t-1}; then the prime totitives of a^t will be given by $\alpha + \lambda a^{t-1}$, $\beta + \lambda a^{t-1}$, &c. where λ has all values from 0 to $a-1$. Now

$$\Pi(x - \overline{\alpha + \lambda a^{t-1}}) \equiv x^a - (C_1^a \alpha + A a^{t-1}) x^{a-1} + (C_2^a \alpha^2 + C_1^{a-1} A a^{t-1} \alpha) x^{a-2} - (C_3^a \alpha^3 + C_2^{a-1} A a^{t-1} \alpha^2) x^{a-3} + \text{&c. mod. } a^t,$$

where the terms containing $\alpha^{2(t-1)}$, $\alpha^{3(t-1)}$, &c. have been dropped, and C_1^a, C_2^a, &c. are the successive binomial coefficients of the a^{th} power, and $A = 0 + 1 + 2 + 3 + \ldots + (a-1) = \frac{a(a-1)}{2}$. But $A \equiv 0 \text{ mod. } a$, $\therefore A a^{t-1} \equiv 0 \text{ mod. } a^t$, and

$$\Pi(x - \overline{\alpha + \lambda a^{t-1}}) \equiv (x - \alpha)^a \text{ mod. } a^t,$$

$$\therefore \Pi_{a^t}(x - \theta_1) \equiv (x-\alpha)^a (x-\beta)^a \ldots (x-\omega)^a \equiv [\Pi_{a^{t-1}}(x - \theta_1)]^a \text{ mod. } a^t.$$

Now,

$$\begin{aligned} \Pi_a(x - \theta_1) &\equiv x^{a-1} - 1 \quad \text{mod. } a, \\ \therefore \Pi_{a^2}(x - \theta_1) &\equiv (x^{a-1} - 1)^a \quad " \quad a^2, \\ \therefore \Pi_{a^3}(x - \theta_1) &\equiv (x^{a-1} - 1)^{a^2} \quad " \quad a^3, \\ \therefore \Pi_{a^t}(x - \theta_1) &\equiv (x^{a-1} - 1)^{a^{t-1}} \quad " \quad a^t, \end{aligned}$$

and the first part of the theorem is proved. The same proof applies to the second part of the theorem, if we suppose α, β, &c. to be not the prime totitives, but the a-totitives of a^{t-1}. Then we get, just as before,

$$\Pi_{a^t}(x - \theta_a) \equiv [\Pi_{a^{t-1}}(x - \theta_a)]^a \text{ mod. } a^t.$$

But we have

$$\begin{aligned} \Pi_a(x - \theta_a) &= x - 0, \\ \therefore \Pi_{a^2}(x - \theta_a) &\equiv x^a \text{ mod. } a^2, \text{ &c.}, \\ \therefore \Pi_{a^t}(x - \theta_a) &\equiv x^{a^{t-1}} \text{ mod. } a^t. \quad \text{Q. E. D.} \end{aligned}$$

If, in the foregoing, we put $a = 2$, then

$$\Pi(x - \overline{\alpha + 2^{t-1}\lambda}) \equiv x^2 - (2\alpha \pm 2^{t-1}) x + (\alpha^2 \pm 2^{t-1}) \text{ mod. } 2^t,$$

since $A = 0 + 1 \equiv \pm 1 \text{ mod. } 2$. This may be written

$$\Pi(x - \overline{\alpha + 2^{t-1}\lambda}) \equiv (x-\alpha)^2 \pm 2^{t-1}(x-1) \text{ mod. } 2^t,$$

$$\therefore \Pi_{2^t}(x - \theta_1) \equiv \{(x-\alpha)^2 \pm 2^{t-1}(x-1)\}\{(x-\beta)^2 \pm 2^{t-1}(x-1)\} \ldots . \{(x-\omega)^2 \pm 2^{t-1}(x-1)\} \text{ mod. } 2^t,$$

$$\therefore \Pi_{2^t}(x - \theta_1) \equiv [\Pi_{2^{t-1}}(x-\alpha)]^2 \pm 2^{t-1}(x-1)\{(x-\beta)^2(x-\gamma)^2 \ldots (x-\omega)^2 + (x-\alpha)^2(x-\gamma)^2 \ldots (x-\omega)^2 + \ldots + (x-\alpha)^2(x-\beta)^2(x-\gamma)^2 \ldots (x-\psi)^2\} \text{mod. } 2^t.$$

Now, if $t > 2$, the number of the prime totitives of 2^{t-1} is even, *i. e.*, α, β, &c. are the 2^{t-2} odd numbers from 1 to $2^{t-1} - 1$. Thus, we have

$$\Pi_{2^t}(x - \theta_1) \equiv [\Pi_{2^{t-1}}(x - \theta_1)]^2 \pm 2^{t-1}(x-1)\{2^{t-2}(x-1)^{2^{t-1}-2} + 2f(x)\} \text{ mod. } 2^t$$

$$\therefore \Pi_{2^t}(x - \theta_1) \equiv [\Pi_{2^{t-1}}(x - \theta_1)]^2 \text{ mod. } 2^t, \text{ when } t > 2.$$

If α, β, γ, &c. be the 2-totitives of 2^{t-1}, *i. e.*, the 2^{t-2} even numbers from 0 to $2^{t-1}-2$, then we get, as before,

$$\Pi_{2^t}(x-\theta_2) \equiv [\Pi_{2^{t-1}}(x-\theta_2)]^2 \pm 2^{t-1}(x-1)\{2^{t-2}x^{2^{t-1}-2} + 2\phi(x)\} \text{ mod. } 2^t$$
$$\therefore\ \Pi_{2^t}(x-\theta_2) \equiv [\Pi_{2^{t-1}}(x-\theta_2)]^2 \text{ mod. } 2^t, \text{ when } t > 2.$$

By inspection, we have

$$\Pi_2(x-\theta_1) = x-1,$$
$$\Pi_4(x-\theta_1) \equiv x^2-1 \text{ mod. } 4,$$
$$\therefore\ \Pi_8(x-\theta_1) \equiv (x^2-1)^2 \text{ mod. } 8,$$

and thence, by induction,

$$\Pi_{2^t}(x-\theta_1) \equiv (x^2-1)^{2^{t-2}} \text{ mod. } 2^t.$$

So we have, by inspection,

$$\Pi_2(x-\theta_2) = x,$$
$$\Pi_4(x-\theta_2) = x(x-2)$$
$$\therefore\ \Pi_8(x-\theta_2) \equiv x^2(x-2)^2 \text{ mod. } 8,$$
$$\therefore\ \Pi_{16}(x-\theta_2) \equiv x^4(x-2)^4 \text{ " } 16,$$
$$\therefore\ \Pi_{2^t}(x-\theta_2) \equiv [x(x-2)]^{2^{t-2}} \text{ mod. } 2^t.$$

This last expression may evidently be written

$$\Pi_{2^t}(x-\theta_2) \equiv x^{2^{t-1}-2}(x^2 + 2^{t-1}x + 2^{t-1}) \text{ mod. } 2^t.$$

Thus we have

Theorem II. If $\Pi(x-\theta_1)$ denote the continued product $(x-\theta_1')(x-\theta_1'')\ldots$, where the numbers θ_1 are the successive odd numbers from 1 to 2^t-1, then, t being > 1,

$$\Pi(x-\theta_1) \equiv (x^2-1)^{2^{t-2}} \text{ mod. } 2^t;$$

and if $\Pi(x-\theta_2)$ denote a similar product where the numbers θ_2 are the successive even numbers from 0 to 2^t-2, then, t being > 2,

$$\Pi(x-\theta_2) \equiv [x(x-2)]^{2^{t-2}} \equiv x^{2^{t-1}-2}(x^2 + 2^{t-1}x + 2^{t-1}) \text{ mod. } 2^t.$$

Example of Theorem I. Suppose $a^t = 27$. Then

$$(x-1)(x-2)(x-4)(x-5)(x-7)(x-8)(x-10)(x-11)(x-13)$$
$$(x+13)(x+11)\ldots(x+1)$$
$$\equiv (x^2-1)(x^2-10)(x^2-19)(x^2-4)(x^2-7)(x^2-16)(x^2-22)(x^2-25)(x^2-13)$$
$$\equiv (x^2-1)^3(x^4-11x^2+1)^3 \equiv (x^6-12x^4+12x^2-1)^3 \equiv (x^2-1)^9 \text{ mod. } 27.$$

That is, $\Pi(x-\theta_1) \equiv (x^2-1)^{3^2}$ mod. 3^3. So,

$$\Pi(x-\theta_3) = (x-0)(x-3)(x-6)\ldots(x+6)(x+3) \equiv x^9 \text{ mod. } 27.$$

Example of Theorem II. Suppose $2^t = 16$. Then

$\Pi(x-\theta_1) = (x-1)(x-3)(x-5)(x-7)(x-9)(x-11)(x-13)(x-15)$
$\equiv (x^2-1)^2(x^2-9)^2 \equiv (x^4-10x^2+9)^2 \equiv x^8-4x^6+6x^4-4x^2+1 = (x^2-1)^4 \text{ mod. } 16.$
So, $(x-0)(x-2)(x-4)(x-6)(x-8)(x+6)(x+4)(x+2) \equiv x^3(x-8)(x^2-4)^2$
$\equiv x^6(x^2+8x+8) \equiv [x(x-2)]^4 \text{ mod. } 16.$

In the following, if $k = a^t b^u \ldots g^v h^w \ldots q^z$, and $s = hi \ldots q$, R_s will denote that one of the roots of $x^2 \equiv x \text{ mod. } k$, which is an s-totitive of k. (For the properties of these roots or repetents, see my paper, Vol. III, No. 4, of this Journal). $R_{\bar{s}}$ will denote that repetent of k whose subscript contains all those prime factors of k not found in s. Thus $R_{\bar{q}}$ will denote briefly the same thing as $R_{ab\ldots p}$. We can now prove the general theorem concerning the function $\Pi_k(x-\theta_s)$ of any integer k.

Theorem III. If $k = a^t b^u \ldots g^v h^w \ldots q^z$, where a, b, &c. are different prime umbers, and if $s = h \ldots q$, $\sigma = h^w \ldots q^z$, and θ_s', θ_s'', &c. be the s-totitives of k, then

$$\Pi_k(x-\theta_s) \equiv R_{\bar{a}}(x^{a-1}-1)^{\tau_{as}(k)} + R_{\bar{b}}(x^{b-1}-1)^{\tau_{bs}(k)} + \ldots + R_{\bar{g}}(x^{g-1}-1)^{\tau_{gs}(k)} + R_{\bar{s}}x^{\tau_s(k)} \text{ mod. } k;$$

except (1) when $\frac{k}{\sigma} = 4$ or a higher power of 2, in which case

$$\Pi_k(x-\theta_s) \equiv R_{\bar{2}}(x^2-1)^{\frac{1}{2}\tau_{2s}(k)} + R_{\bar{s}}x^{\tau_s(k)} \text{ mod. } k,$$

and (2) when $\frac{k}{\sigma} = 1$ and $a^t = 2^t$ where $t =$ or > 2, in which case, if $t = 2$, then

$$\Pi_k(x-\theta_s) \equiv x^{\tau_s(k)} + \tfrac{1}{2}kx^{\tau_s(k)-1} \text{ mod. } k,$$

and if $t > 2$, then

$$\Pi_k(x-\theta_s) \equiv x^{\tau_s(k)} + \tfrac{1}{2}kx^{\tau_s(k)-1} + \tfrac{1}{2}kx^{\tau_s(k)-2} \text{ mod. } k.$$

To prove the theorem, let us consider each component of the modulus separately. With respect to mod. a^t, the formula to be proved reduces to

$$\Pi_k(x-\theta_s) \equiv (x^{a-1}-1)^{\tau_{as}(k)} \text{ mod. } a^t,$$

since $R_{\bar{b}}$, $R_{\bar{c}}$, $\ldots R_{\bar{g}}$, $R_{\bar{s}}$ each contain a^t, and $R_{\bar{a}} \equiv 1$, mod. a^t. Now it is clear that if we take the residues mod. a^t of the numbers θ_s we shall get each prime totitive of a^t the same number of times, and shall consequently get, in all, $\frac{\tau_s(k)}{\tau_1(a^t)}$ groups, each group containing all the prime totitives of a^t. If

$\Pi_a (x - \theta_s)$ denote the product taken for those numbers θ_s which compose any one of these groups, then by Theorem I

$$\Pi_{a^t} (x - \theta_s) \equiv (x^{a-1} - 1)^{a^{t-1}} \text{ mod. } a^t,$$

if a be an odd prime number. Hence

$$\Pi_k (x - \theta_s) \equiv (x^{a-1} - 1)^{a^{t-1} \frac{\tau_s(k)}{\tau(a^t)}} \text{ mod } a^t,$$

or

$$\Pi_k (x - \theta_s) \equiv (x^{a-1} - 1)^{\tau_{as}(k)} \text{ mod. } a^t.$$

If $a = 2$, we have, by Theorem II,

$$\Pi_{2^t} (x - \theta_s) \equiv (x^2 - 1)^{2^{t-2}} \text{ mod. } 2^t,$$

$$\therefore \Pi_k (x - \theta_s) \equiv (x^2 - 1)^{2^{t-2} \frac{\tau_s(k)}{2^{t-1}}} \text{ mod. } 2^t.$$

Now, if $\frac{k}{\sigma}$ contain at least one odd prime number, then $2^{t-2} \cdot \frac{\tau_s(k)}{2^{t-1}} \left(= \frac{1}{2} \tau_{2s}(k) \right)$ is divisible by 2^{t-1}; but $(x^2 - 1)^{2^{t-1}} = (x - 1)^{2^{t-1}} (\overline{x - 1} + 2)^{2^{t-1}}$, and $(\overline{x - 1} + 2)^{2^{t-1}} \equiv (x - 1)^{2^{t-1}}$ mod. 2^t, therefore $(x^2 - 1)^{2^{t-1}} \equiv (x - 1)^{2^t}$ mod. 2^t. Therefore,

$$\Pi_k (x - \theta_s) \equiv (x - 1)^{\tau_{2s}(k)} \text{ mod. } 2^t.$$

But if $\frac{k}{\sigma} = 4$, or a higher power of 2, according to exception (1), then we have, as above,

$$\Pi_k (x - \theta_s) \equiv (x^2 - 1)^{\frac{1}{2}\tau_{2s}(k)} \text{ mod. } 2^t.$$

Having shown that the formula holds true for mod. a^t, we have shown it true for mod. $\frac{k}{\sigma}$, since no distinction is to be made among $a, b, \ldots g$.

Let us now consider one of the components of σ, as q^z. The formula to be proved reduces to

$$\Pi_k (x - \theta_s) \equiv x^{\tau_s(k)} \text{ mod. } q^z,$$

since $R_{\bar{s}} \equiv 1$ mod. q^z, and $R_{\bar{a}} R_{\bar{b}} \ldots R_{\bar{g}}$ each contain q^z. The numbers θ_s all contain q, and it is clear that, if we take their residues mod. q^z, we shall get each q-totitive of q^z the same number of times, and shall consequently get, in all, $\frac{\tau_s(k)}{q^{z-1}}$ groups, each group containing all the q-totitives of q^z. If $\Pi_{q^z} (x - \theta_s)$ denote the product taken for those numbers θ_s which compose any one of these groups, then, by Theorem I, we have, when q is odd,

$$\Pi_{q^z} (x - \theta_s) \equiv x^{q^{z-1}} \text{ mod. } q^z.$$

$$\therefore \Pi_k (x - \theta_s) \equiv x^{\tau_s(k)} \text{ mod. } q^z.$$

But if $q = 2$, we have, by Theorem II, second part,

$$\Pi_{2^z} (x - \theta_s) \equiv (x(x - 2))^{2^{z-2}} \text{ mod. } 2^z.$$

$$\therefore \Pi_k (x - \theta_s) \equiv (x(x - 2))^{\frac{1}{2}\tau_s(k)} \text{ mod. } 2^z.$$

And if $\frac{k}{\sigma}$ be not equal to unity, then $\frac{1}{2}\tau_s(k)$ will be divisible by 2^{z-1} when $q = 2$. Then, since $[x(x-2)]^{2^{z-1}} \equiv x^{2^z} \bmod 2^z$, it follows that

$$\Pi_k(x-\theta_s) \equiv (x)^{\tau_s(k)} \bmod 2^z, \text{ as before.}$$

But if $\frac{k}{\sigma} = 1$ and $q = 2$, then $\frac{\tau_s(k)}{2^{z-1}}$ is odd, and we have, by Theorem II, as before,

$$\Pi_{q^z}(x-\theta_s) \equiv [x(x-2)]^{2^{z-2}} \equiv x^{2^{z-1}-2}(x^2 + 2^{z-1}x + 2^{z-1}) \bmod 2^z,$$

where the last term in the parenthesis is present or absent according as $z > 2$ or $z = 2$.

$$\therefore \Pi_k(x-\theta_s) \equiv [x^{2^{z-1}-2}(x^2 + 2^{z-1}x + 2^{z-1})]^{\frac{\tau_s(k)}{2^{z-1}}} \bmod 2^z.$$

Now, $(x^2 + 2^{z-1}x + 2^{z-1})^n \equiv (x^2)^n + n\{(x^2)^{n-1}(2^{z-1}x) + (x^2)^{n-1}(2^{z-1})\} \bmod 2^z$ which, when n is odd, becomes

$$\equiv x^{2n} + 2^{z-1}x^{2n-1} + 2^{z-1}x^{2n-2} = x^{2n-2}(x^2 + 2^{z-1}x + 2^{z-1}) \bmod 2^z.$$

Then, since $\frac{\tau_s(k)}{2^{z-1}}$ is odd, we have for $z > 2$,

$$\Pi_k(x-\theta_s) \equiv x^{n(2^{z-1}-2)}(x^2 + 2^{z-1}x + 2^{z-1})\, x^{2n-2} \bmod 2^z,$$

where $n = \frac{\tau_s(k)}{2^{z-1}}$. Now, since $\frac{k}{2^z}$ is odd, we have $\frac{1}{2}k = 2^{z-1}(2\lambda + 1)$. Then $2^{z-1} \equiv \frac{1}{2}k \bmod 2^z$.

$$\therefore \Pi_k(x-\theta_s) \equiv x^{\tau_s(k)-2}\left(x^2 + \tfrac{1}{2}kx + \tfrac{1}{2}k\right) \bmod 2^z,$$

which is exception (2), second part. In exactly the same way we get when $z = 2$,

$$\Pi_k(x-\theta_s) \equiv x^{\tau_s(k)-2}\left(x^2 + \tfrac{1}{2}kx\right) \bmod 2^z,$$

which is exception (2), first part.

Having shown, now, that the formula of the theorem holds good with respect to any component of the modulus, the theorem is proved.

In the expansion of $R_{\bar{a}}(x^{a-1}-1)^{\tau_{as}(k)}$ the coefficient of x^r is

$$\equiv (-)^{\frac{\tau_s(k)-r}{a-1}} R_{\bar{a}}\, C_{\frac{r}{a-1}}^{\tau_{as}(k)} \text{ or } = 0,$$

according as r is or is not divisible by $a-1$, where $C_{\frac{r}{a-1}}^{\tau_{as}(k)}$ is a binomial coeffi-

cient. For, if r contain $a-1$, then $(-)^{\tau_{as}(k)-\frac{r}{a-1}} = (-)^{\frac{\tau_s(k)-r}{a-1}}$. Therefore, putting $\tau_s(k)-r=m$, the preceding theorem may be stated as follows:

Theorem IV. If $k = a^t b^u \ldots g^v h^w \ldots q^z$, $s = h \ldots q$, and $P_m(\theta_s)$ denote $\Sigma\theta_s'\theta_h'' \ldots \theta_s^{[m]}$, where θ_s', &c. are the s-totitives of k, then

$$P_m(\theta_s) \equiv \sum_{\omega=a}^{\omega=g} (-)^{\overline{\omega-1}} R_{\bar{\omega}} C^{\tau_{\omega s}(k)}_{\frac{m}{\omega-1}} \text{ mod. } k,$$

the summation including only those terms for which $\frac{m}{\omega-1}$ is an integer; except (1) when $\frac{k}{\sigma} = 4$ or a higher power of 2, in which case

$$P_m(\theta_s) \equiv (-)^{\frac{m}{2}} R_{\bar{2}} C^{\frac{1}{2}\tau_{2s}(k)}_{\frac{m}{2}} \text{ mod. } k,$$

and (2) when $\frac{k}{\sigma} = 1$ and one of the components of $k = 2^n$, in which case, if $n = 2$, then

$$P_1(\theta_s) \equiv \tfrac{1}{2} k, \text{ and } P_{1+\lambda} \equiv 0 \text{ mod. } k,$$

but if $n > 2$, then

$$P_1(\theta_s) \equiv P_2(\theta_s) \equiv \tfrac{1}{2} k, \text{ and } P_{2+\lambda} \equiv 0 \text{ mod. } k.$$

When $m = \tau_s(k)$, the formula becomes

$$P_{\tau_s(k)}(\theta_s) \equiv R_{\bar{a}} + R_{\bar{b}} + \ldots + R_{\bar{g}} \equiv R_{\overline{ab\ldots g}} = R_s \text{ mod. } k,$$

except when $\frac{k}{\sigma} = p^n$, $2p^n$, or 4, and $\frac{\sigma}{s}$ is at the same time an odd number, in which case $\tau_s(k) : p-1$ is odd, and the formula becomes

$$P_{\tau_s(k)}(\theta_s) \equiv -R_s \text{ mod. } k.$$

This special case of the formula is the generalization of the Wilsonian theorem given in my former paper, for $P_{\tau_s(k)}(\theta_s)$ = the product of the s-totitives of k.

Example. Suppose $k = 60 = 2^2 . 3 . 5$, then those three roots of $x^2 \equiv x$ mod. 60 which I have denoted by $R_{\bar{2}}$, $R_{\bar{3}}$, $R_{\bar{5}}$ are 45, 40, 36 respectively.

I. $s = 1$.

$$P_m(\theta_1) \equiv (-)^{\frac{m}{2-1}} R_{\bar{2}} C^{\tau_2(60)}_{\frac{m}{2-1}} + (-)^{\frac{m}{3-1}} R_{\bar{3}} C^{\tau_3(60)}_{\frac{m}{3-1}} + (-)^{\frac{m}{5-1}} R_{\bar{5}} C^{\tau_5(60)}_{\frac{m}{5-1}} \text{ mod. } 60.$$

Whence

$$P_1(\theta_1) \equiv -45 . 16 \equiv 0,$$

$$P_2(\theta_1) \equiv 45 . \frac{16 . 15}{1 . 2} - 40 . 8 \equiv -20,$$

$$P_3(\theta_1) \equiv -45 . \frac{16 . 15 . 14}{1 . 2 . 3} \equiv 0,$$

$$P_4(\theta_1) \equiv 45 . \frac{16 . 15 . 14 . 13}{1 . 2 . 3 . 4} + 40 . \frac{8 . 7}{1 . 2} - 36 . 4 \equiv 16,$$

etc., to $$P_{16}(\theta_1) \equiv R_{\bar{2}} + R_{\bar{3}} + R_{\bar{5}} \equiv 1 .$$

These relations, expressed by Theorem III, become

$$\Pi(x-\theta_1) \equiv R_{\bar{2}}(x-1)^{\tau_2(60)} + R_{\bar{3}}(x^2-1)^{\tau_3(60)} + R_{\bar{5}}(x^4-1)^{\tau_5(60)} \text{ mod. } 60 ,$$

or,

$$\Pi(x-\theta_1) \equiv 45(x-1)^{16} + 40(x^2-1)^8 + 36(x^4-1)^4 \text{ mod. } 60 .$$

II. $s = 5$.

$$P_m(\theta_5) \equiv (-)^{\overline{2-1}} R_{\bar{2}} C^{\tau_{2.5}(60)}_{\overline{\frac{m}{2-1}}} + (-)^{\overline{\frac{m}{3-1}}} R_{\bar{3}} C^{\tau_{3.5}(60)}_{\overline{\frac{m}{3-1}}} \text{ mod. } 60 .$$

$$P_1(\theta_5) \equiv -45.4 \equiv 0 ,$$

$$P_2(\theta_5) \equiv 45.\frac{4.3}{1.2} - 40.2 \equiv 10 ,$$

$$P_3(\theta_5) \equiv -45.\frac{4.3.2}{1.2.3} \equiv 0 ,$$

$$P_4(\theta_5) \equiv 45 + 40 \equiv 25 = R_5 .$$

These relations, when expressed by Theorem III, become

$$\Pi(x-\theta_5) \equiv 45(x-1)^4 + 40(x^2-1)^2 + 36x^4 \text{ mod. } 60 .$$

III. $s = 3$.

$$P_m(\theta_3) \equiv (-)^{\overline{\frac{m}{2-1}}} R_{\bar{2}} C^{\tau_{2.3}(60)}_{\overline{\frac{m}{2-1}}} + (-)^{\overline{\frac{m}{5-1}}} R_{\bar{5}} C^{\tau_{5\ 3}(60)}_{\overline{\frac{m}{5-1}}} \text{ mod. } 60 ,$$

$$P_1(\theta_3) \equiv -45.8 \equiv 0 ,$$

$$P_2(\theta_3) \equiv 45.\frac{8.7}{1.2} \equiv 0 ,$$

$$P_3(\theta_3) \equiv -45.\frac{8.7.6}{1.2.3} \equiv 0 ,$$

$$P_4(\theta_3) \equiv 45.\frac{8.7.6.5}{1.2.3.4} - 36.2 \equiv 18 , \text{ etc., to}$$

$$P_8(\theta_3) \equiv 45 + 36 \equiv 21 = R_3 ; \text{ otherwise,}$$

$$\Pi(x-\theta_3) \equiv 45(x-1)^8 + 40x^8 + 36(x^4-1)^2 \text{ mod. } 60 .$$

IV. $s = 2$.

$$P_m(\theta_2) \equiv (-)^{\overline{\frac{m}{3-1}}} R_{\bar{3}} C^{\tau_{3.2}(60)}_{\overline{\frac{m}{3-1}}} + (-)^{\overline{\frac{m}{5-1}}} R_{\bar{5}} C^{\tau_{5.2}(60)}_{\overline{\frac{m}{5-1}}} \text{ mod. } 60 ,$$

$$P_1(\theta_2) \equiv 0 ,$$

$$P_2(\theta_2) \equiv -40.\frac{8.7}{1.2} \equiv 20 ,$$

$$P_3(\theta_2) \equiv 0 ,$$

$$P_4(\theta_2) \equiv 40.\frac{8.7.6.5}{1.2.3.4} - 36.4 \equiv 16 , \text{ etc., to}$$

$$P_8(\theta_2) \equiv 40 + 36 \equiv 16 = R_2 .$$

V. $s = 2.3$.

$$P_m(\theta_{2.3}) \equiv (-)^{\frac{m}{5-1}} R_{\bar{5}} C^{\tau_{5.2.3}(60)}_{\frac{m}{5-1}} \text{ mod. } 60,$$
$$P_1(\theta_{2.3}) \equiv P_2 \equiv P_3 \equiv 0,$$
$$P_4(\theta_{2.3}) \equiv -36.2 \equiv -12,$$
$$P_5 \equiv P_6 \equiv P_7 \equiv 0,$$
$$P_8(\theta_{2.3}) \equiv 36 = R_{2.3}.$$

VI. $s = 3.5$.

This is a case of exception (1), since $\frac{k}{\sigma} = \frac{60}{3.5} = 4$.

$$\therefore P_m(\theta_{3.5}) \equiv (-)^{\frac{m}{2}} R_{\bar{2}} C^{\frac{1}{2}\tau_{2.3.5}(60)}_{\frac{m}{2}} \text{ mod. } 60,$$
$$P_1 \equiv 0,$$
$$P_2 \equiv -45 = -R_{3.5}.$$

VII. $s = 5.2$.

$$P_m(\theta_{5.2}) \equiv (-)^{\frac{m}{3-1}} R_{\bar{3}} C^{\tau_{3.5.2}(60)}_{\frac{m}{3-1}} \text{ mod. } 60,$$
$$P_1 \equiv P_3 \equiv 0,$$
$$P_2(\theta_{5.2}) \equiv -40.2 = -20,$$
$$P_4(\theta_{5.2}) \equiv 40 \cdot \frac{2.1}{1.2} = R_{5.2}.$$

VIII. $s = 2.3.5$.

This is a case of exception (2), since $\frac{k}{\sigma} = \frac{60}{2^2.3.5} = 1$, and 60 contains 4.

$$\therefore P_1(\theta_{2.3.5}) \equiv \frac{1}{2}(60), \text{ and } P_2 \equiv 0 = R_{2.3.5}.$$

The only two numbers included here are

$$0 \text{ and } 30, \; P_1 = 0 + 30, \text{ and } P_2 = 0.30.$$

Theorem V. If $k = a^t b^u \ldots q^z$, and $\Pi_k(x - \theta)$ denote the continued product, $x(x-1)(x-2)\ldots(x-\overline{k-1})$, then

$$\Pi_k(x - \theta) \equiv R_{\bar{a}}(x^a - x)^{\frac{k}{a}} + R_{\bar{b}}(x^b - x)^{\frac{k}{b}} + \ldots + R_{\bar{q}}(x^q - x)^{\frac{k}{q}} \text{ mod. } k;$$

except when one of the factors of k, as a, $= 2$, and $t > 1$, in which case

$$\Pi_k(x - \theta) \equiv R_{\bar{2}}[(x^2 - x)^2 - 2(x^2 - x)]^{\frac{k}{4}} + R_{\bar{b}}(x^b - x)^{\frac{k}{b}} + \ldots + R_{\bar{q}}(x^q - x)^{\frac{k}{q}} \text{ mod. } k.$$

To prove this theorem we have only to consider one component of the modulus, as a^t. Since $R_{\bar{b}}$, $R_{\bar{c}}$, ... $R_{\bar{q}}$ each contain a^t, and $R_{\bar{a}} \equiv 1$ mod. a^t, the congruence to be proved reduces to $\Pi_k(x - \theta) \equiv (x^a - x)^{\frac{k}{a}}$ mod. a^t. Now it is

evident that if we take the residues of the successive numbers less than k, we shall get $\frac{k}{a^t}$ successive groups. According to Theorem I, $\Pi(x-\theta)$ for one group $\equiv (x^a - x)^{a^{t-1}}$ mod. a^t. Therefore, $\Pi_k(x-\theta) \equiv (x^a - x)^{\frac{k}{a}}$ mod. a^t. But if $a=2$, and $t>1$, then $\Pi(x-\theta)$ for one group $\equiv [(x^2-1)(x^2-2x)]^{2^{t-2}}$ mod. 2^t, according to Theorem II. Therefore,

$$\Pi_k(x-\theta) \equiv [(x^2-1)(x^2-2x)]^{\frac{k}{4}} \equiv [(x^2-x)^2 - 2(x^2-x)]^{\frac{k}{4}} \text{ mod. } 2^t. \quad \text{Q. E. D.}$$

By comparing the coefficients of corresponding powers of x, we have the residues, mod. k, of the symmetric functions $\Sigma\alpha$, $\Sigma\alpha\beta$, &c. of the successive numbers from 0 to $k-1$ in terms of the repetents or residual units of k. When k does not contain 4, we may write the theorem more simply as follows, dispensing with the "carrier," x:

$$P_m(\theta) \equiv \sum_{\omega=a}^{\omega=q} (-)^{\frac{m}{\omega-1}} R_{\bar{\omega}} C^{\frac{k}{\omega}}_{\frac{m}{\omega-1}} \text{ mod. } k,$$

where C is a binomial coefficient, and where only those terms are to be included in the summation for which m is divisible by $\omega - 1$. But if $k = 2^t b^u c^v \ldots q^z$, and $t > 2$, then it is easy to show that

$$P_m(\theta) \equiv (-)^m R_{\bar{2}} \left(C^{\frac{k}{2}}_m + \frac{k}{2} C^{\frac{k}{2}-1}_{m-2} + \frac{k}{2} C^{\frac{k}{2}-2}_{m-4} \right) + \sum_{\omega=b}^{\omega=q} (-)^{\frac{m}{\omega-1}} R_{\bar{\omega}} C^{\frac{k}{\omega}}_{\frac{m}{\omega-1}} \text{ mod. } k.$$

If $t=2$, the last term in the parenthesis is to be omitted; if $t=1$, the last two terms in the parenthesis are to be omitted, and the formula is then included under the preceding formula.

For example, suppose $k=30$, and it is required to find the residue mod. 30 of $P_4(\theta)$. We have $R_{\bar{2}} = 15$, $R_{\bar{3}} = 10$, and $R_{\bar{5}} = 6$. Then

$$P_4(\theta) \equiv (-)^4 R_{\bar{2}} C^{15}_4 + (-)^2 R_{\bar{3}} C^{10}_2 + (-)^1 R_{\bar{5}} C^6_1 \text{ mod. } 30,$$

or
$$P_4(\theta) \equiv 15 \cdot \frac{15.14.13.12}{1.2.3.4} + 10 \cdot \frac{10.9}{1.2} - 6 \cdot \frac{6}{1} \text{ mod. } 30,$$

or
$$P_4(\theta) \equiv 15 + 0 - 6 \equiv 9 \text{ mod. } 30.$$

Since, now, the value of any symmetric function whatever can be obtained by means of the tables explicitly in terms of the symmetric functions $\Sigma\alpha$, $\Sigma\alpha\beta$, $\Sigma\alpha\beta\gamma$, &c. we have thus a means of expressing, in terms of the repetents of k, the residues mod. k of any symmetric function of the s-totitives of k, or, finally, of any symmetric function of the successive numbers from 0 to $k-1$.

§ 2. *Extension of Preceding Results to the Theory of Functions (mod. p, $f(x)$).*

Let $f(x) = K \equiv A^t B^u \ldots Q^z$ mod. p, where p is a prime number, t, u, &c. are any integers, and A, B, &c. are irreducible (mod. p) functions of x, of

forms $x^a + \lambda_1 x^{a-1} + \lambda_2 x^{a-2} +$ &c., $x^b + \mu_1 x^{b-1} + \mu_2 x^{b-2} +$ &c., &c. respectively. It is well known that K can be so represented in only one way.

A function, $\phi(x)$, is said to contain another function, $f(x)$, *with respect to* p, when $\phi(x) = f(x)f_1(x) + pf_2(x)$. In the following the words *with respect to* p are always to be understood when the word *contain* is used with reference to functions, and when one function is said to be prime to another it is to be understood that they have no common factor *with respect to* p.

Let the number of incongruous (mod. p) functions of a less degree than that of K and prime to K be called the prime totient of K, and let it be denoted by $\tau_1(K)$ after the analogy of Professor Sylvester's notation and nomenclature in the case of integers. Likewise let the functions themselves be called the prime totitives of K. In the same way let the number of those which contain A but no other prime factor of K be called the A-totient of K, and let it be denoted by $\tau_A(K)$; and let the functions themselves be called the A-totitives of K. So on, for $\tau_{AB}(K)$, $\tau_{ABC}(K)$, &c. There are plainly 2^i different classes of totitives of K, if i denote the number of the unequal prime factors of K. A means of finding the value of the different totients of K will be furnished by the following:

Lemma. There are p^{n-m} *incongruous (mod.* p*) functions of* x*, degree* $< n$*, which contain a given function* $\phi(x)$ *of form* $x^m + \lambda_1 x^{m-1} + \lambda_2 x^{m-2} + \ldots + \lambda_m$.

For let $\psi(x) = \alpha x^{n-1} + \beta x^{n-2} +$ &c., where α, β, &c. are variable coefficients. Dividing $\psi(x)$ by $\phi(x)$, we get a remainder of degree $m - 1$. In order that there may be an exact division, each of the coefficients of the remainder must be equal to zero. We thus have m equations, which, as the process of division shows, are linear in the n quantities, α, β, &c. We may give arbitrary values to $n - m$ of these quantities, and considering the system of equations as a system of congruences mod. p, we may evidently satisfy the system in p^{n-m} different ways. Hence the *lemma* is proved.

Suppose, now, that $K = A^t B^u C^v$. We easily find, by means of the preceding lemma, and by use of the process employed to find the totients of an integer, that

$$\begin{aligned}
\tau_1(K) &= p^{(t-1)a} p^{(u-1)b} p^{(v-1)c} (p^a - 1)(p^b - 1)(p^c - 1), \\
\tau_A(K) &= \quad " \qquad\quad " \qquad\quad (p^b - 1)(p^c - 1), \\
\tau_{AB}(K) &= \quad " \qquad\quad " \qquad\quad\quad (p^c - 1), \text{ &c.}
\end{aligned}$$

The analogy between these numbers and the totients of an integer is at once apparent, viz: if an integer $k = a^t b^u c^v$ where a, b, c are prime numbers, the totients of K are derived from the totients of k by substituting in the latter

p^a for a, p^b for b, &c., where, however, a, b, c, the degrees of A, B, C, are not prime numbers, but any integers.

It is proposed, in what follows, to show briefly that certain theorems of my former paper, as well as those of the preceding section, have their analogues in the theory of functions (mod. p, K).

Let us first consider the properties of the roots of $X^2 \equiv X$ (mod. p, K), where $K = A^t B^u \ldots G^v H^w \ldots Q^z$. Let $s = H \ldots Q$, and $\sigma = H^w \ldots Q^z$. We evidently have $X \equiv 0$ (mod. p, σ), and $X \equiv 1 \left(\text{mod. } p, \frac{K}{\sigma}\right)$, and thence $\lambda\sigma - \mu \frac{K}{\sigma} \equiv 1$ mod. p. Since σ and $\frac{K}{\sigma}$ have no common factor with respect to p, this congruence gives one, and only one, value of λ. (See Serret, *Cours d'Alg. Sup.*, § 341), and consequently one, and only one, value of X for the two preceding congruences. This value contains σ. Call it R_s. It is evident now that there are twice as many roots of $X^2 \equiv X$ (mod. p, K) as there are ways of separating K into two factors prime to one another, viz: 2^i, and that one of them belongs to each of the 2^i classes of the totitives of K, where i is the number of the unequal prime factors in K. It is at once evident that these roots or repetents of K have the same properties as the integer roots of $x^2 \equiv x$ mod. k. For convenience, I restate some of them:

(1). $R_s R_{s'} \equiv R_{ss'}$ (mod. p, K), where s and s' are prime to each other.

(2). The sum of any given number of the repetents of K is congruous (mod. p, K) to the sum of the same number of any others of them, provided only that the product of the subscripts is the same for each sum.

(3). If $\bar{s}$ denote the product of all the unequal prime factors of K *not* contained in s, then

$$R_{\bar{s}} R_{\bar{s}'} \equiv 0 \text{ (mod. } p, K),$$

(4). $R_{\bar{s}} + R_{\bar{s}'} + \ldots + R_{\bar{s}^{[n]}} \equiv R_{\overline{ss'\ldots s^{[n]}}}$ (mod. p, K).

(5). If A', B', $\ldots$ G' be prime totitives of A^t, B^u, $\ldots$ G^v, respectively, and H', $\ldots$ Q' are multiples of H, I, $\ldots$ Q, respectively, then the residue (mod. p, K) of the function, $A'R_{\bar{A}} + B'R_{\bar{B}} + \ldots + Q'R_{\bar{Q}}$ is an s-totitive of K.

The analogue of Fermat's extended theorem is $X_s^{\tau_s(K)} \equiv R_s$ (mod. p, K), where X_s is an s-totitive of K.

If $K = A^t$, it is proved, in the ordinary way, that

$$X_1^{\tau_1(A^t)} \equiv 1 \text{ (mod. } p, K),$$

and it is, of course, obvious that

$$X_A^{\tau_A(A^t)} \equiv 0 \text{ (mod. } p, K).$$

Hence the theorem is true for $K = A^t$, since $R_1 = 1$ and $R_A = 0 \pmod{p, K}$. Then since [see (5)]

$$X_s \equiv A'R_{\overline{A}} + B'R_{\overline{B}} + \ldots + Q'R_{\overline{Q}} \pmod{p, K},$$

we have, by raising both sides to power $\tau_s(K)$, inasmuch as $\tau_s(K)$ contains $\tau_1(A^t), \ldots \tau_1(G^v)$,

$$X_s^{\tau_s(K)} \equiv R_{\overline{A}} + R_{\overline{B}} + \ldots + R_{\overline{G}} \equiv R_{\overline{AB\ldots G}} = R_s \pmod{p, K};$$

and the general theorem is proved.

Let it be required now to find the residues (mod. p, K) of the symmetric functions $\Sigma\Theta_s'$, $\Sigma\Theta_s'\Theta_s''$, &c., where Θ_s', Θ_s'', &c. are the s-totitives of K, or, in other words, to find the residue of the function $\Pi_K(X - \Theta_s)$, in analogy with the results of the preceding section. First, let us prove that $\Pi_{A^t}(X - \Theta_1) \equiv [\Pi_{A^{t-1}}(X - \Theta_1)]^{p^\alpha} \pmod{p, A^t}$. The method of proof is precisely that of last section. Let α, β, γ, &c. be the prime totitives of A^{t-1}; then those of A^t will be given by $\alpha + \lambda A^{t-1}$, $\beta + \lambda A^t$, &c. where λ is any one of the p^α incongruous (mod. p) functions of a less degree than that of A. But

$$\Pi(X - \overline{\alpha + \lambda A^{t-1}}) \equiv X^{p^\alpha} - (C_1^{p^\alpha}\alpha + \Omega A^{t-1})X^{p^\alpha - 1} + (C_2^{p^\alpha}\alpha^2 + C_1^{p^\alpha}\Omega A^{t-1}\alpha)X^{p^\alpha - 2} - (C_3^{p^\alpha}\alpha^3 + C_2^{p^\alpha - 1}\Omega A^{t-1}\alpha^2)X^{p^\alpha - 3} + \&c. \pmod{p, A^t}$$

just as before, where Ω here equals the sum of the p^α incongruous (mod. p) functions of a less degree than that of A. But we evidently have $\Omega \equiv 0 \bmod p$.

$$\therefore \Pi(X - \overline{\alpha + \lambda A^{t-1}}) \equiv (X - \alpha)^{p^\alpha}, \pmod{p, A^t}.$$
$$\therefore \Pi_{A^t}(X - \Theta_1) \equiv [(X - \alpha)(X - \beta)\ldots]^{p^\alpha}, \pmod{p, A^t}.$$
$$\therefore \Pi_{A^t}(X - \Theta_1) \equiv [\Pi_{A^{t-1}}(X - \Theta_1)]^{p^\alpha}, \pmod{p, A^t}.$$

Now we know (*Serret*, § 345, *et seq.*) that

$$\Pi_A(X - \Theta_1) \equiv X^{p^\alpha - 1} - 1, \pmod{p, A},$$
$$\therefore \Pi_{A^2}(X - \Theta_1) \equiv (X^{p^\alpha - 1} - 1)^{p^\alpha}, \pmod{p, A^2},$$
$$\therefore \Pi_{A^t}(X - \Theta_1) \equiv (X^{p^\alpha - 1} - 1)^{p^{\alpha(t-1)}}, \pmod{p, A^t}.$$

In the same way, we evidently get

$$\Pi_{A^t}(X - \Theta_A) \equiv (X)^{p^{\alpha(t-1)}}, \pmod{p, A^t}.$$

In general we have the following

Theorem. If $K = A^tB^u \ldots G^vH^w \ldots Q^z$, where A, B, &c. are different irreducible (mod. p) functions of x, of degrees, a, b, &c. and if $S = HI \ldots Q$, and Θ_s', Θ_s'', &c. be the S-totitives of K, then

$$\Pi_K(X - \Theta_S) \equiv R_{\overline{A}}(X^{p^\alpha - 1} - 1)^{\tau_{AS}(K)} + \ldots + R_{\overline{G}}(X^{p^\gamma - 1} - 1)^{\tau_{GS}(K)} + R_{\overline{S}}X^{\tau_S(K)}, \pmod{p, K}.$$

There are no exceptions to this formula as in the case of the corresponding formula for integers, for the unique prime number, 2, has no analogue in this theory of functions. The proof of the theorem is so nearly the same as that of the one for integers that it does not seem worth while to repeat it here. It is simply a substitution of p^a for a, p^b for b, &c. and (mod. p, K) for mod. k in the proof of Theorem III in the last section.

If $P_m(\Theta_s)$ denote $\Sigma\Theta_s'\Theta_s'' \ldots \Theta_{s^{(r)}}^{[m]}$, we have as another form of the preceding theorem, analogous to Theorem IV of the last section,

$$P_m(\Theta_s) \equiv \sum_{\Omega=A}^{\Omega=G} (-)^{\frac{m}{\tau(\Omega)}} R_{\bar{\Omega}} C_{\frac{m}{\tau(\Omega)}}^{\frac{\tau_s(K)}{\tau(\Omega)}}, \text{ mod. } (p, K),$$

where the process of summation includes only those terms for which $\frac{m}{\tau(\Omega)}$, *i. e.*, $\frac{m}{p^\omega - 1}$ = an integer.

When $m = \tau_s(K)$, the formula becomes

$$P_{\tau_s(K)} \equiv R_{\bar{A}} + R_{\bar{B}} + \ldots + R_{\bar{G}} \equiv R_{\overline{AB\ldots G}} = R_S,$$

except when $\frac{K}{\sigma}$ = a power of an irreducible function, as A^t, and p is not 2, in which case $\frac{\tau_s(K)}{\tau(A)}$, *i. e.* $\frac{\tau_s(K)}{p^a - 1}$, is odd, and we have

$$P_{\tau_s(K)} \equiv -R_{\bar{A}} = -R_S, \text{ (mod. } p, K).$$

Since $P_{\tau_s(K)}$ = the product of the s-totitives of K, this special case of the above theorem constitutes the analogue of the generalized Wilsonian theorem.

It is easy to see that Theorem V of last section also has its analogue here, viz: If $\Pi_K(X - \Theta)$ denote the continued product $(X - \Theta')(X - \Theta'') \ldots$ where Θ', Θ'', &c. are the whole set of the $\varkappa = p^{a+b+\cdots+q}$ incongruous (mod. p, K) functions of x from 0 up to K, then

$$\Pi_K(X - \Theta) \equiv R_{\bar{A}}(X^{p^a} - X)^{\frac{\kappa}{p^a}} + \ldots + R_{\bar{Q}}(X^{p^q} - X)^{\frac{\kappa}{p^q}}, \text{ [mod. } p, K],$$

or

$$P_m(\Theta) \equiv (-)^{\frac{m}{p^a-1}} R_{\bar{A}} C_{\frac{m}{p^a-1}}^{\frac{\kappa}{p^a}} + \ldots + (-)^{\frac{m}{p^q-1}} R_{\bar{Q}} C_{\frac{m}{p^q-1}}^{\frac{\kappa}{p^q}}, \text{ (mod. } p, K).$$

BALTIMORE, 14 *April*, 1881.